AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Jason M. Guyton, being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent with Homeland Security Investigations (HSI), currently assigned to HSI Cleveland, Ohio. I have been employed with HSI since March 2009. As part of my daily duties as an HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251(a), 2252(a) and 2252A(a). I have received training in child pornography and child exploitation investigations and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I teach how to conduct child exploitation investigations to new agents at the HSI Academy and have presented at multiple national conferences related to these investigations. I have written numerous affidavits in support of search and arrest warrants related to investigations of child pornography, online enticement, and other child exploitation crimes. I am a federal law enforcement officer authorized by the Secretary of Homeland Security to request the issuance of search warrants.

2. The statements in this affidavit are based upon my personal knowledge and observations, my training and experience, information obtained from other law enforcement and witnesses, and the review of various documents and records. Because this affidavit is being

submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth the facts that I believe necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a) are present in the information associated with the Dropbox account(s) associated with the following user:

Email Address: mckainchris3@gmail.com

Screen/Username: Chris Mckain

ESP USER ID: 1811023569

I make this affidavit in support of an application for a search warrant for content and records associated with the above accounts which are stored at a premise owned, maintained, controlled, or operated by Dropbox Inc. ("Dropbox"), an online storage provider headquartered at 1800 Ownes Street, San Francisco, CA 94158.

3. The information and accounts to be searched is described in the following paragraphs and in Attachments A and B. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Dropbox to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts referenced in this affidavit and further in Attachment A, including the contents of the account.

4. I have probable cause to believe that evidence of violations of 18 U.S.C. § 2252A, involving the use of a computer in or affecting interstate commerce to transport, receive, distribute,

possess and/or access child pornography is located within the accounts described below. I have reason to believe that the member accounts that are the subject of the instant application will have stored information and communications that are relevant to this investigation, to include evidence of the identity of the person maintaining the account and other relevant information associated with the user. Thus, as outlined below, and based on my training and experience, there is probable cause to believe that evidence, fruits and/or instrumentalities of the crimes are in these accounts.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of Title 18, United States Code, §2252A, and relating to material involving the sexual exploitation of minors. 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, distributing, receiving, reproducing for distribution, possessing or accessing with intent to view any child pornography, as defined in 18 U.S.C. §2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

6. The legal authority for this search warrant application is derived from Title 18, United States Code, chapter 121, §§ 2701-11, entitled "Stored Wire and Electronic Communications and Transactional Records Access." 18 U.S.C. § 2703(c)(A) allows for nationwide service of process of search warrants for the contents of electronic communications. Pursuant to 18 U.S.C. § 2703, as amended by the USA PATRIOT Act, Section 220, a government entity may require a provider of an electronic communication service or a remote computing service to disclose a record

or other information pertaining to a subscriber or customer of such service pursuant to a warrant issued using procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation. 18 U.S.C. § 2510(12) defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo optical system that affects interstate or foreign commerce," with certain exceptions not applicable here. 18 U.S.C. § 2510(17) defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

DEFINITIONS

7. The following definitions apply to this Affidavit and its Attachments:

   a. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

   b. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

c. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

d. The term "child pornography," as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where

i. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

ii. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

iii. such visual depiction has been created, adapted, or modified to

appear that an identifiable minor is engaging in sexually explicit conduct.

e. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as flash drives, SD cards, floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), optical disks, printer buffers, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

f. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

g. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies a computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. A creation IP address is the address used on the date that an e-mail account is created by the user.

h. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

i. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

j. A "Preservation Letter" is a letter government entities issue to Internet providers pursuant to 18 U.S.C. § 2703(f) to ensure that the Internet Providers preserve records in its possession. The preservation of such records is necessary given the dynamic nature of digital records that may be deleted.

k. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

l. A "hash value" is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

BACKGROUND ON DROPBOX AND INTERNET PROTOCOL (IP) ADDRESSES

8. Dropbox refers to an online storage medium on the Internet accessed from a computer or electronic storage device. As an example, online storage mediums such as Dropbox make it possible for the user to have access to saved files without the requirement of storing said files on their own computer or other electronic storage device. Dropbox is an "offsite" storage medium for data that can be viewed at any time from any device capable of accessing the internet. Users can store their files on Dropbox and avoid having the files appear on their computer. Anyone searching an individual's computer that utilizes Dropbox would not be able to view these files if

the user opted only to store them at an offsite such as Dropbox. These are often viewed as advantageous for collectors of child pornography in that they can enjoy an added level of anonymity and security.

9. Dropbox is a file hosting service operated by Dropbox, Inc., headquartered in San Francisco, California, that offers cloud storage, file synchronization, personal cloud, and client software. Dropbox allows users to create a special folder on each of their computers, which Dropbox then synchronizes so that it appears to be the same folder (with the same contents) regardless of which computer is used to view it. Files placed in this folder also are accessible through a website and mobile phone applications. Each Dropbox user is afforded 2GB of free storage space that may be used to save photographs, videos, documents, and e-mail messages. Users can manually upload and sync the files on their computer to the Dropbox account or they can set their account to automatically sync files to the Dropbox account after a certain amount of time. The frequency with which someone uploads files to their Dropbox account may be different for each user. For this reason, users may have received and retained files in their regular email account for some time prior to uploading or syncing the files to the Dropbox storage.

10. Dropbox provides a variety of online services, including online storage access, to the public. Dropbox allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other

identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

11. When the subscriber transfers a file to a Dropbox account, it is initiated at the user's computer, transferred via the Internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. This includes online storage in Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.

12. Online storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in times and durations (i.e., session), the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

13. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

14. I know from my training and experience that Dropbox preserves the content of the accounts that have been flagged, or at the request of a law enforcement agency preservation request.

INFORMATION REGARDING NCMEC

15. The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a private, non-profit organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further their mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the Cyber Tipline and Child Victim Identification Programs. NCMEC makes information submitted to the Cyber Tipline and Child Victim Identification Programs available to law enforcement and uses this information to help identify trends and create child safety and prevention messages. As a national clearinghouse, NCMEC also works with Electronic Service Providers (ESPs), law enforcement, and the public in a combined effort to reduce online child sexual abuse images. NCMEC does not act in the capacity of or under the direction or control of the government or any

law enforcement agency. NCMEC does not independently investigate and cannot verify the accuracy of the information submitted by reporting parties.

16. Cyber Tipline Reports are initially submitted to NCMEC. Anyone can submit a Cyber Tipline Report, although the majority of Cyber Tipline Reports your Affiant reviews are submitted by ESPs such as Google, Facebook, Instagram, Yahoo, Microsoft, Dropbox, and the like. Cyber Tipline Reports from ESPs typically contain information about the subscriber, such as the subscriber's username, email address, telephone numbers, and IP address history. Cyber Tipline Reports will also contain the child sexual abuse material (CSAM) that caused the ESP to initiate the report. That CSAM is often image or video files of child pornography as defined by federal law.

STATEMENT OF PROBABLE CAUSE

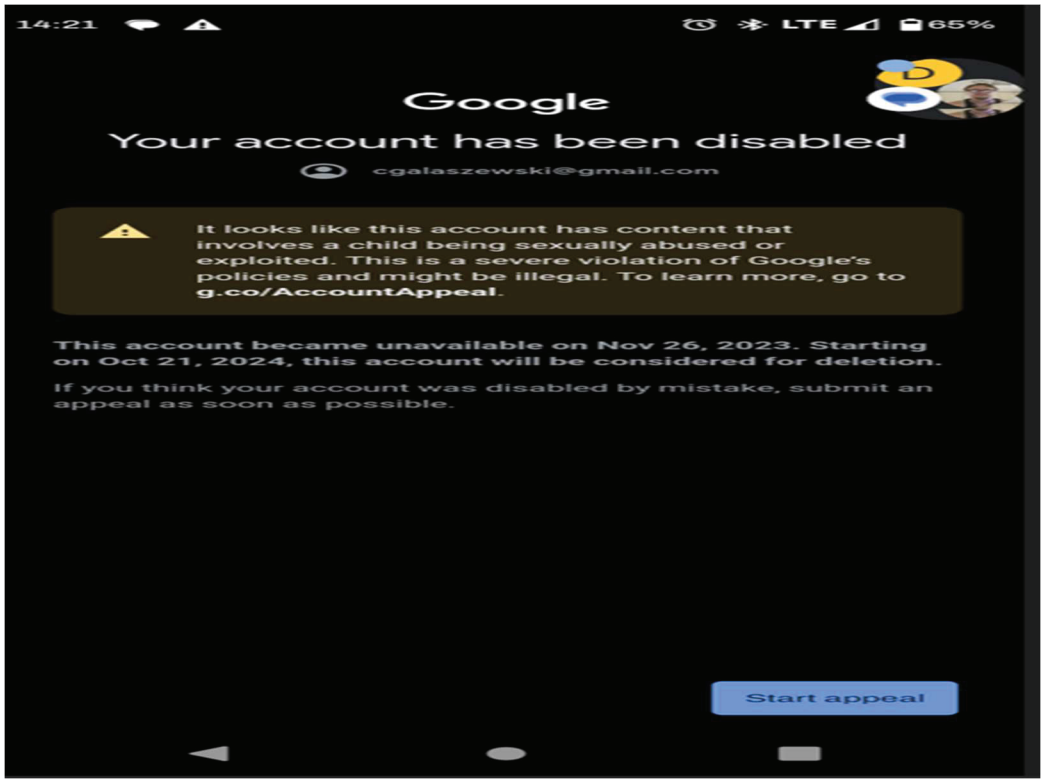
17. In September 2023, your Affiant began investigating Christopher GALASZEWSKI, a registered sex offender, for distributing files depicting suspected child sexual abuse material (CSAM) using an online messaging application that was being monitored by law enforcement. GALASZEWSKI was previously incarcerated by the State of Ohio from 08/07/2018 to 06/09/2023 for convictions related to Rape (Ohio Revised Code 2907.02 5) and Gross Sexual Imposition (Ohio Revised Code 2907.05.5). Your Affiant learned that at the time of this investigation GALASZEWSKI was on active Parole/Supervision with Ohio Adult Parole Authority (APA) Officer Brendan Centeno. Further, your Affiant learned that GALASZEWSKI was arrested by Officer

Centeno on November 28, 2023, and subsequently returned to prison for violating terms of his Parole/Supervision (Expected release date is 08/23/2024).

18. Officer Centeno provided a copy of his Violation Report for GALASZEWSKI to your Affiant for review. In this report, Officer Centeno wrote that on November 26, 2023, he received multiple text messages and phone calls from GALASZEWSKI stating that his second phone (216-290-8900) had been hacked. Officer Centeno described GALASZEWSKI as "very nervous", and wrote that GALASZEWSKI stated, "he didn't do anything and that there was child porn on his Gmail account (cgalaszewski@gmail.com) because it was hacked". When Officer Centeno asked what exactly was on the phone, GALASZEWSKI stated, "a couple pictures but that he had deleted them". Officer Centeno instructed GALASZEWSKI not to touch or delete anything on the phone and scheduled a meeting with him (**NOTE:** Your Affiant confirmed with Officer Centeno that when GALASZEWSKI contacted him on this day, he was residing at the City Mission located at XXXX Carnegie Avenue, Cleveland, Ohio 44103).

19. Officer Centeno's Violation Report indicated that he met GALASZEWSKI at the City Mission in Cleveland on November 28, 2023, and GALASZEWSKI admitted to having over 100 pictures of child pornography on his Android cellphone. Further, GALASZEWSKI showed Officer Centeno where they were located on the device. Officer Centeno reviewed some of these files and confirmed that they depicted what he identified as child pornography. During his arrest of GALASZEWSKI, Officer Centeno seized an iPhone, Android phone, and an HP laptop from him.

20. On February 22, 2024, your Affiant obtained a search warrant from United States Magistrate Judge Thomas M. Parker (Case No. 1:24-mj-3019 TMP) in the United States District Court for the Northern District of Ohio to search the electronic devices that Officer Centeno seized from GALASZEWSKI. While reviewing the electronic contents of a Motorola, Moto G Play, cellphone (IMEI # 359687212362090) pursuant to this warrant your Affiant observed numerous user attributes and activity (to include selfie style pictures) that linked it to GALASZEWSKI. Further, your Affiant observed that the user of this cellphone sent the following image using text message to "C Blue", "Mom", and "Dad":



In conjunction with this image, your Affiant observed a text reading "I am going to prison" was sent to "C Blue" on 11/26/2023 at 7:23:59 PM (UTC +0). The individual pictured in the upper right-hand corner of this file matches multiple images of GALASZEWSKI that your Affiant has seen. Lastly, while reviewing this device, your Affiant observed multiple files of suspected CSAM including the lascivious exhibition of child's genitals, as well as at least one (1) file depicting a toddler being sexually penetrated by an adult male's erect penis.

21. On March 22, 2024, your Affiant asked Ohio Internet Crimes Against Children (ICAC) Task Force Criminal Analyst (C/A) Caroline Wathey to conduct a check of the ICAC Data System (IDS) for the email address cgalaszewski@gmail.com, that was displayed in the image pictured in paragraph 20. IDS is a database that allows law enforcement to see if any number of unique identifiers, to include email addresses, have been previously associated with an ICAC investigation involving CSAM. The IDS database also checks to see if these unique identifiers are associated with any NCMEC Cyber Tipline Reports. This check indicated that this email address was associated with a Cyber Tipline Report that was previously made to NCMEC.

22. On November 27, 2023, the Electronic Service Provider (ESP) Google submitted Cyber Tipline (CT) Report 180609808 to NCMEC regarding the possible possession, manufacture, and/or distribution of child pornography by the following user:

Name:	Christopher Galasezwski
Phone:	+12164234688 (Verified 11-16-2023)

	+14409411745 (Verified 07-29-2023) +12162908900 (Verified 09-06-2023)
Date of Birth:	06-16-1998
Email Address:	cgalaszewski@gmail.com (Verified) mckainchris3@gmail.com
ESP User ID:	RGQXX2MYHJVIQ65YG262CHWWUI

Google reported that on November 26, 2023, this user uploaded seventeen (17) files of apparent child pornography over the Google Gmail infrastructure. Google reported these files were uploaded on November 26, 2023, between 18:40:50 hours UTC and 18:41:11 hours UTC from IP address that resolved to Cleveland, Ohio.

23. On March 28, 2024, Ohio ICAC Intake Officer (I/A) Nicole Reedy provided your Affiant with an additional Cyber Tipline Report associated with **mckainchris3@gmail.com**, the additional email address that Google provided with their Cyber Tip. This report indicated that on June 13, 2023, the ESP Dropbox submitted Cyber Tipline Report #164084798 to NCMEC regarding the possible possession, manufacture, and/or distribution of child pornography by the following user:

Email Address:	mckainchris3@gmail.com (Verified 06-13-2023 23:56:10 UTC)
Screen/User Name:	Chris Mckain
ESP User ID:	1811023569
IP Address:	2607:fb90:b530:4967:a646:3a5:53cc:f2a5 (Registration) 06-13-2023 23:56:09 UTC

Dropbox reported that on June 12, 2023, this user uploaded two (2) files of apparent child pornography to this Dropbox account. Dropbox, after viewing the content of all these files, provided them to NCMEC as part of their Cyber Tip. An initial check of the IP address used to by **Chris McKain** to upload these files resolved to T-Mobile USA in the Cleveland-Akron metro area. Your Affiant knows that the phones utilized by GALASZEWSKI during this investigation were registered to T-Mobile.

24. On April 1, 2024, your Affiant reviewed the content of the files provided by Dropbox as part of the Cyber Tip they submitted. Your Affiant observed that the user of this account added the submitted files to a folder labeled "HideU" on their account. One of the files your Affiant viewed can be more fully described as follows:

a. File Name 509EE473.jpge" depicts a fully nude prepubescent female leaning back against a log with her legs spread looking directly at the camera. The child's genital area is clearly visible to the camera. There is a watermark on the image that reads "www.BD-COMPANY.com", and there are four smaller images that appear to depict additional prepubescent females in various states of undress.

25. Based on the above information, your Affiant has probable cause to believe that the Dropbox user **Chris Mckain**, using email address **mckainchris3@gmail.com**, committed the offense of possessing and/or distributing child pornography, in violation of Title 18, United States Code, §§2252A and that information contained within this account and maintained at Dropbox will

assist law enforcement in identifying the person or persons using this account. In addition, your Affiant knows that as part of their policy when submitting Cyber Tips to NCMEC, that Dropbox preserves the contents of the reported account so it is anticipated that the account will contain additional evidence that is relevant to this investigation.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

26. Your Affiant anticipates executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

27. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in control of Dropbox there exists evidence of a crime, contraband and/or fruits of a crime. Based on the aforementioned information, I respectfully submit that there is probable cause to believe that the Dropbox account described in Attachment A will contain evidence of a crime, specifically but not limited to, identification of the person who possessed and/or distributed files of child pornography through the Dropbox account discussed above. Accordingly, a search warrant is requested.

28. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(I).

29. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Because the warrant will be served on Dropbox, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Jason M. Guyton
Special Agent
Homeland Security Investigations

Sworn to via telephone after submission by reliable electronic means [Fed. R. Crim. P. 4.1 and 41(d)(3)] on this 4th day of April 2024.

REUBEN J. SHEPERD
UNITED STATES MAGISTRATE JUDGE